

DORA skærper krav til cybersikkerheden og til ledelsens ansvar

DORA er på vej til den finansielle sektor med formålet om at forbedre cybersikkerheden i EU. Forordningen skal skabe klarhed over reglerne, reducere virksomhedernes administrative byrder samt sikre et passende sikkerhedsniveau i alle medlemsstater. Den 17. januar 2025 finder de nye regler anvendelse, og det medfører et nyt ansvarsområde for ledelsen.

Det er direktionen og bestyrelsen, som har ansvaret for at overholde DORA-reglerne. Det vil sige de personer, som er udpeget i overensstemmelse med national lovgivning, der har mandat til at fastlægge enhedens strategi, målsætninger og generelle ledelsesprincipper, og som fører tilsyn med ledelsens beslutningstagning. Det omfatter personer, som varetager enhedens daglige ledelse.

Direktionen og bestyrelsen er ansvarlige for at fastlægge, føre tilsyn med og gennemføre alle ordninger, der vedrører rammerne for IKT-risikostyring. De ansvarlige er pålagt at besidde den viden og de færdigheder, som er nødvendige for at forstå og vurdere IKT-risici samt deres indvirkning på den finansielle enheds drift, herunder ved regelmæssigt at følge særlige kurser svarende til den IKT-risiko, der styres.

OVERHOLDES KRAVENE IKKE, KAN LEDELSEN HOLDES ANSVARLIG FOR:

- Overtrædelser, jf. DORA.
- Pligtforsømmelser, jf. selskabsloven og lov om finansiell virksomhed.
- Tilsynet kan få flere beføjelser, men skal som minimum have disse:
 - Påbud om at ophøre adfærd og afholde sig fra at gentage den.
- Midlertidigt eller permanent forbud mod praksis eller adfærd.
- Enhver foranstaltning, herunder af økonomisk karakter, til at sikre, at selskabet overholder sine forpligtelser.
- Udsendelse af offentlige meddelelser, herunder offentlige erklæringer, der angiver ledelsens identitet og karakteren af deres overtrædelser.